arXiv:cs/0605139v1 [cs.CR] 30 May 2006

Construction and Count of Boolean Functions of an Odd Number of Variables with Maximum Algebraic Immunity *

Na Li, Wen-Feng Qi
Department of Applied Mathematics, Zhengzhou
Information Engineering University
P.O.Box 1001-745, Zhengzhou, 450002,
People's Republic of China
E-mail: mylina_1980@yahoo.com.cn, wenfeng.qi@263.net

Abstract

Algebraic immunity has been proposed as an important property of Boolean functions. To resist algebraic attack, a Boolean function should possess high algebraic immunity. It is well known now that the algebraic immunity of an n-variable Boolean function is upper bounded by $\lceil \frac{n}{2} \rceil$. In this paper, for an odd integer n, we present a construction method which can efficiently generate a Boolean function of n variables with maximum algebraic immunity, and we also show that any such function can be generated by this method. Moreover, the number of such Boolean functions is greater than $2^{2^{n-1}}$.

Keywords. Algebraic attacks, algebraic immunity, annihilators, Boolean functions.

1 Introduction

Recently, Algebraic attack has gained a lot of attention in cryptanalysing stream and block cipher systems [1]-[5]. The study on algebraic attack adds an important property of Boolean functions to be used in cryptosystems,

*This work was supported by the National Natural Science Foundation of China (Grant 60373092).

which is known as algebraic immunity. Possessing high algebraic immunity is a necessary requirement for a Boolean function when used in a cryptosystem. Now, it is known that the algebraic immunity of an n-variable Boolean function is upper bounded by $\lceil \frac{n}{2} \rceil$ [2].

Boolean functions with maximum algebraic immunity are an important class of Boolean functions, and there is an increasing interest in construction of such Boolean functions. In [6], D. K. Dalai *et al.* first presented a construction method which can generate some Boolean functions with maximum algebraic immunity. This construction provides only one high dimension Boolean function from a low dimension Boolean function, so it can provide only a few of such Boolean functions. Then, a construction [7] keeping in mind the basic theory of annihilator immunity was presented. In [8], the authors gave three construction methods which each can get a class of Boolean functions with maximum algebraic immunity from one such given function. Several classes of symmetric Boolean functions of an even number of variables with maximum algebraic immunity were presented in [9]. However, the number of symmetric Boolean functions given by them is small. Moreover, it was showed that there exists only one symmetric Boolean function (besides its complement) of an odd number of variables with maximum algebraic immunity [10]. So far, there is no literature which pointed out that how many on earth such Boolean functions are and how one can construct an arbitrary such function.

In this paper, for an odd integer n, we convert the problem of finding an n-variable Boolean function with maximum algebraic immunity to the problem of finding a $k \times k$ invertible submatrix of a $2^{n-1} \times 2^{n-1}$ invertible matrix. Thereby we present a construction method which can efficiently generate an n-variable Boolean function with maximum algebraic immunity, and we also show that any such function can be constructed by this method. Finally, we show that the number of such Boolean functions is equal to the number of $k \times k$ invertible submatrixes of a $2^{n-1} \times 2^{n-1}$ invertible matrix, and thus the number of Boolean functions of an odd number of variables with maximum algebraic immunity is greater than $2^{2^{n-1}}$.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the set of all n-tuples of elements in the finite field $\mathbb{F}_2$. To avoid confusion with the usual sum, we denote the sum over $\mathbb{F}_2$ by $\oplus$.

A Boolean function of n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Any Boolean function f of n variables can be uniquely represented as

$$f(x_1,\ldots,x_n)=a_0\oplus\sum_{1\le i\le n}a_ix_i\oplus\sum_{1\le i<j\le n}a_{i,j}x_ix_j\oplus\ldots\oplus a_{1,\ldots,n}x_1x_2\ldots x_n,$$

where the coefficients $a_0, a_i, a_{i,j}, \ldots, a_{1,\ldots,n} \in \mathbb{F}_2$. And such form of f is called the algebraic normal form (ANF) of f. The algebraic degree, $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient. The Boolean function f can also be identified by its truth table which is the vector of length 2^n consisting of the function values. The set of $X \in \mathbb{F}_2^n$ for which $f(X) = 1$ (resp. $f(X) = 0$) is called the onset (resp. offset), denoted by 1_f (resp. 0_f). The cardinality of 1_f is called the Hamming wight of f, denoted by $wt(f)$. We say that an n-variable Boolean function f is balanced if $wt(f) = 2^{n-1}$. Let $S = (s_1, s_2, \ldots, s_n) \in \mathbb{F}_2^n$, the Hamming weight of S, denoted by $wt(S)$, is the number of 1's in $\{s_1, s_2, \ldots, s_n\}$.

Definition 1 [11]. *For a given n-variable Boolean function f, a nonzero n-variable Boolean function g is called an annihilator of f if $f \cdot g = 0$, and the algebraic immunity (AI) of f, denoted by $AI(f)$, is the minimum value of d such that f or $f \oplus 1$ admits an annihilating function of degree d.*

An important step in the algebraic attack is to find out low degree annihilators of a Boolean function or its complement. Thus in order to resist algebraic attacks, neither the Boolean function nor its complement used in a cryptosystem should have an annihilator of low degree. That is, the Boolean function should have high algebraic immunity. In the next section, we will present a construction method to generate Boolean functions of an odd number of variables which achieve the maximum algebraic immunity.

3 Construction and Count

Let f be a Boolean function of n variables, and

$$1_f = \{X_1, \ldots, X_{wt(f)}\}, 0_f = \{X_{wt(f)+1}, \ldots, X_{2^n}\}.$$

It is clear that an n-variable Boolean function g is an annihilator of f if and only if $1_f \subseteq 0_g$. For $X = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, we let

$$v(X) = (1, x_1, \ldots, x_n, x_1x_2, \ldots, x_{n-1}x_n, \ldots\ldots, x_1\cdots x_{\lceil \frac{n}{2} \rceil -1}, \ldots, x_{\lfloor \frac{n}{2} \rfloor +2}\cdots x_n),$$

which belongs to $\mathbb{F}_2^{\sum_{i=0}^{\lceil \frac{n}{2} \rceil -1}\binom{n}{i}}$. Let $V(1_f)$ be the $wt(f) \times \sum_{i=0}^{\lceil \frac{n}{2} \rceil -1}\binom{n}{i}$ matrix with row vectors $v(X_1), \ldots, v(X_{wt(f)})$ and $V(0_f)$ the $(2^n - wt(f)) \times \sum_{i=0}^{\lceil \frac{n}{2} \rceil -1}\binom{n}{i}$ matrix with row vectors $v(X_{wt(f)+1}), \ldots, v(X_{2^n})$.

Lemma 1. *Let f be a Boolean function of n variables. Then $AI(f) = \lceil \frac{n}{2} \rceil$ if and only if the ranks of $V(1_f)$ and $V(0_f)$ are both $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$.*

Proof. If there exists a linear relationship among the columns of $V(1_f)$ (resp. $V(0_f)$), then an annihilator of f (resp. $f \oplus 1$) with degree less than $\lceil \frac{n}{2} \rceil$ can be found. On the other hand, if there is an annihilator of f (resp. $f \oplus 1$) with degree less than $\lceil \frac{n}{2} \rceil$, then there must exist a linear relationship among the columns of $V(1_f)$ (resp. $V(0_f)$). Therefore, $\mathrm{AI}(f) = \lceil \frac{n}{2} \rceil$ if and only if the ranks of $V(1_f)$ and $V(0_f)$ are both $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$. □

Note that for odd integer n, $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i} = 2^{n-1}$, and any n-variable Boolean function with maximum algebraic immunity must be balanced [12]. Furthermore, such functions have the following property.

Lemma 2. *[13] Let odd integer $n = 2t + 1$, and f be an n-variable balanced Boolean function. If f does not have any annihilator with degree less than $t + 1$, then $f \oplus 1$ has no annihilator with degree less than $t + 1$. Consequently, $AI(f) = t + 1$.*

Corollary 1. *Let odd integer $n = 2t+1$ and f be an n-variable Boolean function. Then, $AI(f) = t + 1$ if and only if f is balanced and $V(1_f)$ is invertible.*

Lemma 3. *[7][9] Let odd integer $n = 2t + 1$ and f be an n-variable Boolean function which satisfies*

$$f(X) = \begin{cases} a & if \ \ wt(X) \leq t \\ a \oplus 1 & if \ \ wt(X) > t \end{cases},$$

where $a \in \mathbb{F}_2$, then $AI(f) = t + 1$.

Remark 1. *If $a = 1$, we denote the function described in Lemma 3 by G_n.*

Let odd integer $n = 2t + 1$, F_n be a Boolean function of n variables with maximum algebraic immunity (for example, $F_n = G_n$), and we may let

$$1_{F_n} = \{Y_1, \ldots, Y_{2^{n-1}}\}, 0_{F_n} = \{Z_1, \ldots, Z_{2^{n-1}}\}.$$

Then $V(1_{F_n})$ and $V(0_{F_n})$ are both $2^{n-1} \times 2^{n-1}$ square matrixes, and their row vectors are $v(Y_1), \ldots, v(Y_{2^{n-1}})$ and $v(Z_1), \ldots, v(Z_{2^{n-1}})$ respectively. By Lemma 1, $V(1_{F_n})$ and $V(0_{F_n})$ are both invertible matrixes. It is clear that a

Boolean function f is balanced if and only if there exist some integer $0 \leq k \leq 2^{n-1}$, integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$ and integers $1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$, such that

$$1_f = \{Z_{i_1}, \ldots, Z_{i_k}\} \cup 1_{F_n} \backslash \{Y_{j_1}, \ldots, Y_{j_k}\}$$

and

$$0_f = \{Y_{j_1}, \ldots, Y_{j_k}\} \cup 0_{F_n} \backslash \{Z_{i_1}, \ldots, Z_{i_k}\}.$$

So, for some integer $1 \leq k \leq 2^{n-1}$, if we can find some integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$ and integers $1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$, such that the $2^{n-1} \times 2^{n-1}$ matrix with the set of row vectors $\{v(Z_{i_1}), \ldots, v(Z_{i_k})\} \cup V(1_{F_n}) \backslash \{v(Y_{j_1}), \ldots, v(Y_{j_k})\}$ is invertible, then by Corollary 1, we can construct a balanced n-variable Boolean function $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}(X)$ with maximum algebraic immunity as follows

$$f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}(X) = \begin{cases} F_n(X) \oplus 1 & \text{if } X \in \{Z_{i_1}, \ldots, Z_{i_k}, Y_{j_1}, \ldots, Y_{j_k}\} \\ F_n(X) & \text{else} \end{cases}. \quad (1)$$

This is the core idea of our construction. The following is a basic conclusion of vector space.

Lemma 4. *Let U be an m-dimension vector space with $m \geq 2$, $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$ two bases of U. Then, for integer $1 \leq k \leq m-1$ and integers $1 \leq i_1 < \ldots < i_k \leq m$, there always exist some integers $1 \leq j_1 < \ldots < j_{m-k} \leq m$, such that*

$$\{\alpha_{i_1}, \ldots, \alpha_{i_k}, \beta_{j_1}, \ldots, \beta_{j_{m-k}}\}$$

is also a base of U.

Corollary 2. *Let odd integer $n = 2t+1$, F_n be a Boolean function of n variables with maximum algebraic immunity and $1_{F_n} = \{Y_1, \ldots, Y_{2^{n-1}}\}, 0_{F_n} = \{Z_1, \ldots, Z_{2^{n-1}}\}$. Then, for any integer $1 \leq k \leq 2^{n-1}-1$ and integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$, there always exist some integers $1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$, such that $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = t+1$, where $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is defined by (1).*

Proof. Since $V(1_{F_n})$ and $V(0_{F_n})$ are both invertible, then $\{v(Y_1), \ldots, v(Y_{2^{n-1}})\}$ and $\{v(Z_1), \ldots, v(Z_{2^{n-1}})\}$ are two bases of 2^{n-1}-dimension vector space $\mathbb{F}_2^{2^{n-1}}$. By Lemma 4, for any integer $1 \leq k \leq 2^{n-1}-1$ and integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$, there always exist some integers $1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$, such that $\{v(Z_{i_1}), \ldots, v(Z_{i_k})\} \cup V(1_{F_n}) \backslash \{v(Y_{j_1}), \ldots, v(Y_{j_k})\}$ is a base of $\mathbb{F}_2^{2^{n-1}}$. That is, the matrix with the set of row vectors $\{v(Z_{i_1}), \ldots, v(Z_{i_k})\} \cup V(1_{F_n}) \backslash \{v(Y_{j_1}), \ldots, v(Y_{j_k})\}$ is invertible. Therefore $\mathrm{AI}(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = t+1$. □

Next, we show how to find those $1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$ for given $1 \leq k \leq 2^{n-1} - 1$ and $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$.

A useful matrix $W(F_n)$. Let odd integer $n = 2t + 1$, F_n be a Boolean function of n variables with maximum algebraic immunity and $1_{F_n} = \{Y_1, \ldots, Y_{2^{n-1}}\}, 0_{F_n} = \{Z_1, \ldots, Z_{2^{n-1}}\}$. Set

$$W(F_n) = V(0_{F_n})V(1_{F_n})^{-1}.$$

Then $W(F_n)$ is a $2^{n-1} \times 2^{n-1}$ invertible matrix. Denote the 2^{n-1} row vectors of $W(F_n)$ by $w(F_n)_1, \ldots, w(F_n)_{2^{n-1}}$. From the definition of $W(F_n)$, we have $V(0_{F_n}) = W(F_n)V(1_{F_n})$, that is,

$$\begin{pmatrix} v(Z_1) \\ v(Z_2) \\ \ldots \\ v(Z_{2^{n-1}}) \end{pmatrix} = \begin{pmatrix} w(F_n)_1 \\ w(F_n)_2 \\ \ldots \\ w(F_n)_{2^{n-1}} \end{pmatrix} \begin{pmatrix} v(Y_1) \\ v(Y_2) \\ \ldots \\ v(Y_{2^{n-1}}) \end{pmatrix}.$$

The following theorem is one of our main result.

Let $W(F_n)_{(i_1,\ldots,i_k)}$ denote the $k \times 2^{n-1}$ matrix with row vectors $w(F_n)_{i_1}, \ldots, w(F_n)_{i_k}$ and $W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ denote the $k \times k$ matrix with column vectors equal to the $j_1th, \ldots, j_kth$ columns of $W(F_n)_{(i_1,\ldots,i_k)}$.

Theorem 1. *Let odd integer $n = 2t + 1$, F_n be a Boolean function of n variables with maximum algebraic immunity and $1_{F_n} = \{Y_1, \ldots, Y_{2^{n-1}}\}, 0_{F_n} = \{Z_1, \ldots, Z_{2^{n-1}}\}$. Then, the set*

$$\{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)} | k = 0, \ldots, 2^{n-1}, 1 \leq i_1 < \ldots < i_k \leq 2^{n-1}, \\ 1 \leq j_1 < \ldots < j_k \leq 2^{n-1}, W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)} \text{ is invertible}\}$$

consists of all n-variable Boolean functions with maximum algebraic immunity, where $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is defined by (1) and $W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is defined as above.

Proof. Since an n-variable Boolean function f with maximum algebraic immunity must be balanced, then f must be of the form $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$. Denote the remaining elements of 1_{F_n} (resp. 0_{F_n}) excluding $Y_{j_1}, \ldots, Y_{j_k}$ (resp. $Z_{i_1}, \ldots, Z_{i_k}$) by $Y'_{k+1}, \ldots, Y'_{2^{n-1}}$ (resp. $Z'_{k+1}, \ldots, Z'_{2^{n-1}}$). Then $V(1_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}})$ is a $2^{n-1} \times 2^{n-1}$ matrix with row vectors

$$v(Z_{i_1}), \ldots, v(Z_{i_k}), v(Y'_{k+1}), \ldots, v(Y'_{2^{n-1}}).$$

By Corollary 1, $\mathrm{AI}(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = t+1$ if and only if $V(1_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}})$ is invertible. Therefore, it is sufficient to prove that $V(1_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}})$ is invertible if and only if $W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible.

Let M denote the $k \times (2^{n-1}-k)$ matrix with column vectors equal to the remaining columns of $W(F_n)_{(i_1,\ldots,i_k)}$ which is defined as above, such that

$$\begin{pmatrix} v(Z_{i_1}) \\ \ldots \\ v(Z_{i_k}) \end{pmatrix} = W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)} \begin{pmatrix} v(Y_{j_1}) \\ \ldots \\ v(Y_{j_k}) \end{pmatrix} \oplus M \begin{pmatrix} v(Y'_{k+1}) \\ \ldots \\ v(Y'_{2^{n-1}}) \end{pmatrix}.$$

Then, we have

$$\begin{pmatrix} v(Z_{i_1}) \\ \ldots \\ v(Z_{i_k}) \\ v(Y'_{k+1}) \\ \ldots \\ v(Y'_{2^{n-1}}) \end{pmatrix} = \begin{pmatrix} W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)} & & M & \\ & 1 & & \\ 0 & & \ldots & \\ & & & 1 \end{pmatrix} \begin{pmatrix} v(Y_{j_1}) \\ \ldots \\ v(Y_{j_k}) \\ v(Y'_{k+1}) \\ \ldots \\ v(Y'_{2^{n-1}}) \end{pmatrix}. \quad (2)$$

From (2), it is obvious that $V(1_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}})$ is invertible if and only if the matrix

$$\begin{pmatrix} W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)} & & M & \\ & 1 & & \\ 0 & & \ldots & \\ & & & 1 \end{pmatrix} \quad (3)$$

is invertible. Further, the matrix (3) is invertible if and only if $W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible. Thus the proof is completed.

□

Remark 2. *Since $W(F_n)$ is a $2^{n-1} \times 2^{n-1}$ invertible matrix, for any integer $1 \le k \le 2^{n-1}-1$ and integers $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, the rank of the $k \times 2^{n-1}$ matrix $W(F_n)_{(i_1,\ldots,i_k)}$ is k, which means there must exist some integers $1 \le j_1 < \ldots < j_k \le 2^{n-1}$ (we note that there may exist many groups of these integers) such that $W(F_n)_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible. We can also derive Corollary 2 by this fact.*

In order to efficiently generate Boolean functions of an odd number of variables with maximum algebraic immunity, we should choose those F_n such that $W(F_n)$ can be efficiently obtained. We note that G_n is such a function. Now, we explain how to obtain the matrix $W(G_n)$. We denote the elements

of 1_{G_n} and 0_{G_n} by some special symbols. Let $Y_{(b_1,\ldots,b_i)} = (y_1,\ldots,y_n) \in 1_{G_n}$, where $1 \le b_1 < \ldots < b_i \le n$. The symbol $Y_{(b_1,\ldots,b_i)}$ means that $wt(Y_{(b_1,\ldots,b_i)}) = i$ and $y_s = 1$ only for $s = b_1,\ldots,b_i$. Let $Y_{(0)}$ denote $(0,\ldots,0)$. Similarly, let $Z_{(a_1,\ldots,a_l)} = (z_1,\ldots,z_n) \in 0_{G_n}$, where $1 \le a_1 < \ldots < a_l \le n$. The symbol $Z_{(a_1,\ldots,a_l)}$ means that $wt(Z_{(a_1,\ldots,a_l)}) = l$ and $z_s = 1$ only for $s = a_1,\ldots,a_l$. It is clear that $wt(Z_{(a_1,\ldots,a_l)}) \ge t+1$ since $Z_{(a_1,\ldots,a_l)} \in 0_{G_n}$. Then, the vector $v(Z_{(a_1,\ldots,a_l)})$ can be expressed as a linear combination of the row vectors of $V(1_{G_n})$ as follows.

$$\begin{aligned} v(Z_{(a_1,\ldots,a_l)}) = c_0 & \sum_{\{b_1,\ldots,b_t\}\subseteq\{a_1,\ldots,a_l\}} v(Y_{(b_1,\ldots,b_t)}) \\ \oplus\, c_1 & \sum_{\{b_1,\ldots,b_{t-1}\}\subseteq\{a_1,\ldots,a_l\}} v(Y_{(b_1,\ldots,b_{t-1})}) \\ \oplus\, c_2 & \sum_{\{b_1,\ldots,b_{t-2}\}\subseteq\{a_1,\ldots,a_l\}} v(Y_{(b_1,\ldots,b_{t-2})}) \oplus \ldots \\ \oplus\, c_i & \sum_{\{b_1,\ldots,b_{t-i}\}\subseteq\{a_1,\ldots,a_l\}} v(Y_{(b_1,\ldots,b_{t-i})}) \oplus \ldots \\ \oplus\, c_{t-1} & \sum_{\{b_1\}\subseteq\{a_1,\ldots,a_l\}} v(Y_{(b_1)}) \oplus c_t v(Y_{(0)}), \end{aligned} \tag{4}$$

where

$$c_0 = 1;$$

$$c_i = 1 \oplus c_0\binom{l}{i} \oplus c_1\binom{l}{i-1} \oplus \ldots \oplus c_{i-1}\binom{l}{1}.$$

From (4), we get the corresponding row vector of $W(G_n)$. And the other row vectors of $W(G_n)$ can also be obtained by this method.

Now, we derive our important result.

Construction. Let odd integer $n = 2t+1$, $1_{G_n} = \{Y_1,\ldots,Y_{2^{n-1}}\}, 0_{G_n} = \{Z_1,\ldots,Z_{2^{n-1}}\}$. To find a Boolean function of n variables with maximum algebraic immunity, what one has to do is the following steps.

Step 1: Select randomly an integer $1 \le k \le 2^{n-1}-1$ and k integers $1 \le i_1 < \ldots < i_k \le 2^{n-1}$;

Step 2: Using Gauss elimination on the column vectors of $W(G_n)_{(i_1,\ldots,i_k)}$, find a group of integers $1 \le j_1 < \ldots < j_k \le 2^{n-1}$, such that the $j_1th,\ldots,j_kth$ column vectors of $W(G_n)_{(i_1,\ldots,i_k)}$ are linear independent.

We construct the Boolean function $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ as follows.

$$f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}(X) = \begin{cases} G_n(X) \oplus 1 & \text{if } X \in \{Z_{i_1}, \ldots, Z_{i_k}, Y_{j_1}, \ldots, Y_{j_k}\} \\ G_n(X) & \text{else} \end{cases}. \tag{5}$$

Then $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ achieves the maximum algebraic immunity $t+1$.

Remark 3. *(i) By Theorem 1, it is clear that any Boolean function of an odd number of variables with maximum algebraic immunity can be constructed by our method.*

(ii)Since AI(f)=AI($f \oplus 1$), The range of value of k in Step 1 only needs to be $1 \leq k \leq 2^{n-2}$.

(iii)For a small k, one can efficiently generate an n-variable Boolean function with maximum algebraic immunity. For example, when $k = 1$, *we first select randomly an integer* $1 \leq i \leq 2^{n-1}$ *according to Step 1. then according to Step 2, we can select any integer* $1 \leq j \leq 2^{n-1}$ *such that the jth element of* $w(G_n)_i$ *is* 1. *Thus we generate a Boolean function* $f_{(i;j)}$.

Finally, we get a result on the count of Boolean functions of an odd number of variables with maximum algebraic immunity.

Theorem 2. *Let n be an odd integer, then the number of n-variable Boolean functions with maximum algebraic immunity is equal to the number of* $k \times k$ *invertible submatrixes of* $W(G_n)$. *Further, it is greater than* $2^{2^{n-1}}$.

Proof. It is clear that for different groups of integers $(i_1, \ldots, i_k; j_1, \ldots, j_k)$, the Boolean functions defined by (5) are different.

By Theorem 1, the first conclusion is obvious. By Corollary 2 and Remark 3, it is clear that the number of n-variable Boolean functions with maximum algebraic immunity is greater than

$$\binom{2^{n-1}}{0} + \binom{2^{n-1}}{1} + \ldots + \binom{2^{n-1}}{2^{n-1}} = 2^{2^{n-1}}.$$

□

4 Conclusion

In this paper, we present a construction method which can efficiently generate a Boolean function of an odd number of variables which possesses maximum algebraic immunity, and we show that any such function can be generated by this method. Based on the construction, we show that the number of this kind of Boolean functions is greater than $2^{2^{n-1}}$. This value is great enough

to reveal that this kind of Boolean functions are numerous. There are some other problems worth studying. For example, how to construct and count Boolean functions of an even number of variables with maximum algebraic immunity, how to construct and count Boolean functions with maximum algebraic immunity keeping in mind of other cryptographic properties such as nonlinearity, propagation and resiliency.

References

[1] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Advances in Cryptology - ASIACRYPT 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, pp. 267-287.

[2] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology – EUROCRYPT 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, pp. 345-359.

[3] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology –CRYPTO 2003(Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, pp. 176-194.

[4] F. Armknecht, and M. Krause, "Algebraic attacks on combiners with memory," in *Advances in Cryptology –CRYPTO 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, pp. 162-175.

[5] F. Armknecht, "Improving fast algebraic attacks," in *FSE 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, pp. 65-82.

[6] D. K. Dalai, K. C. Gupta and S. Maitra, "Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity," in *FSE 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2005, pp. 98-111.

[7] D. K. Dalai, S. Maitra and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," in *Design, Codes and Cryptography*. Accepted.

[8] L.Qu, G.Feng and C.Li, "On the Boolean functions with maximum possible algebraic immunity: construction and a lower bound of the count," http://eprint.iacr.org/2005/449.pdf.

[9] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," in *INDOCRYPT 2005 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2005, pp. 35-48.

[10] Na Li and Wen-Feng Qi, "Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity," in *IEEE Trans.Inf.Theory*. Accepted.

[11] W. Meier, E. Pasalic and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology –EUROCRYPT 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, pp. 474-491. Germany: Springer-Verlag, 2004, pp. 92-106.

[12] D. K. Dalai, K. C. Gupta and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions," in *INDOCRYPT 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, pp. 92-106.

[13] A.Canteaut, "Open problems related to algebraic attacks on stream ciphers," in *WCC 2005*. Invited talk. pp. 1-10.